Alerta de seguridad informática	2CMV23-00418-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de junio de 2023
Última revisión	09 de junio de 2023

PARA EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO LEER ACÁ

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) ha identificado una nueva campaña de phishing con malware, suplantando a BancoEstado con un falso aviso de pago.

Sí la victima interactúa con este falso documento ejecuta dos códigos maliciosos los cuales son Modiloader y Remcos. Modiloader es un programa que se encarga de realizar las múltiples etapas en la carga útil del malware, mientras que Remcos se usa para obtener información, posee funciones de keylogger, puede grabar el micrófono y hacer capturas de pantalla, además de tomar control del equipo infectado.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
797a26c77e77386595b546a20e2654c9e7c2c14294390a2e2a9eee715b9a392c	Aviso de pago del Banco del Estado.img
b5336f410d43416162e091970d023d3d4f6b93276bbeab99412056dfc1a78aa2	BANCO_DE.EXE

URL-Dominio

Dominio	Relación
http://savory.com[.]bd/imagify-backup/167_Hpxmebnuzgs	Configuración del Malware
193.239.84[.]153:9184	Comando y Control
217.16.85[.]25	SMTP
info@znidarsic[.]si	Correo de Salida

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.002
Ejecución (Ejecución del usuario)	T1204.002
Descubrimiento (Consulta de Registro)	T1012
Descubrimiento (Información del Sistema)	T1082
Comando y Control (Codificación de datos)	T1132.001

Imagen del Mensaje

¡Notificación de pago bancario entrante!

BD Banco del Estado <lab4@[redacted].mk>
Para carias@interior.gov.cl

Responder | Responder a todos | Reenviar | ...

mi. 07/06/2023 9:42

Aviso de pago del Banco del Estado.img
1 MB

Estimado [redacted]

Este aviso de pago se emite a petición de nuestro cliente. Su cuenta bancaria corporativa que termina en ***** ha sido acreditada con un pago interno

Consulte el documento de pago adjunto para obtener más detalles [redacted] del tercero que recibió el pago.

Saludos,

Departamento de Remesas
Banco del Estado
Sede: Chile
[redacted]

FALSO
CSIRT

Este correo electrónico es solo para fines informativos y no está listo para aceptar respuestas. Por lo tanto, le agradecemos que no responda a esta dirección. Declaración de confidencialidad
Este mensaje y los documentos que lo acompañan son confidenciales y son para uso exclusivo de la persona o entidad a quien va dirigido, por lo que el Banco del Estado no se hace responsable del conocimiento de su contenido por parte de terceros.

Si usted no es el destinatario de este mensaje, se le informará que ha recibido el mensaje por error y cualquier uso, distribución, reenvío u otra divulgación, impresión o reproducción de este mensaje está expresamente prohibido y debe eliminarlo inmediatamente de su sistema y Destruirlo con todos sus anexos y notificar al Banco del Estado de la situación.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.06.09 19:06:48 -04'00'